January 11, 2021

Trisha Anderson
Deputy Assistant Secretary for Intelligence and Security
US Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Via e-mail to ICTsupplychain@doc.gov (RE: RIN 0605–AA62)

Ms. Anderson,

BSA | The Software Alliance[1] appreciates the opportunity to provide the below comments to the Department of Commerce's Notice of Proposed Rulemaking (NPRM) on Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications (RIN 0605-AA62). This NPRM implements Executive Order (EO) 14034 on Protecting Americans' Sensitive Data from Foreign Adversaries,[2] signed by President Biden in July 2021, and proposes to clarify the US Department of Commerce's Interim Final Rule (IFR) published in January 2021, which implements EO 13873 on Securing the Information and Communications Technology and Services Supply Chain,[3] signed by President Trump in May 2019.

BSA is the leading advocate for the global enterprise software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, providing

[1] BSA's members include: Adobe, Atlassian, Alteryx, Autodesk, Bentley Systems, Box, CNC/Mastercam, CrowdStrike, DocuSign, Dropbox, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries | The White House, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/.

[3] Executive Order on Securing the Information and Communications Technology and Services Supply Chain | The White House, available at https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

the products and services that power governments and businesses. BSA members are also leaders in security, having pioneered many of the software security best practices used throughout the industry today, including The BSA Framework for Secure Software. BSA also provided specific recommendations on supply chain security in its recent white paper, Building a More Effective Strategy for ICT Supply Chain Security, which advocates a shift to an assurance-based approach built on policies that are (1) cohesive and wholistic; (2) risk-based; (3) narrowly tailored; (4) acceptable when applied reciprocally; (5) transparent, including offering clear routes to adjudicate adverse actions; and (6) subject to robust public consultation and frequent review.

As a preliminary matter, it remains unclear how the numerous US Government EOs, task forces, and similar efforts focused on supply chain security are coordinated. To the extent the Department of Commerce and the US Government more generally, can communicate and strengthen coordination across these efforts, it would improve industry's ability to partner with the US Government and foster progress on the US Government's desired security outcomes.

The Underlying Interim Final Rule Remains Too Broad to Meet the Security Objectives

In BSA's March 22 comments, BSA recommended several concrete improvements that would make the IFR more effective. In short, BSA recommended:

1. Developing and implementing voluntary licensing procedures prior to enforcing the IFR;
2. Tailoring the rules to apply only where necessary to address an identified threat and where concrete and articulable security benefits will outweigh the political, economic, and other costs of this extraordinary intervention in the commercial market;
3. Adopting a criticality assessment methodology as part of the tailored approach to determine which transactions to review;
4. Limiting the scope of review to transactions in which a foreign adversary has a controlling interest;
5. Modifying related definitions;
6. Excluding low risk and non-domestic transactions; and
7. Incorporating procedural safeguards.

In addition, BSA recommends that the Department of Commerce harmonize US Government reviews to eliminate duplication. For instance, to the extent a transaction could otherwise be subject to review by the Committee on Foreign Investment in the United States, the Department should ensure there are not multiple reviews.

The NPRM Does Not Address Underlying Concerns with the IFR's Approach

The NPRM, (a) recognizes explicitly that "connected software applications" are part of ICTS and (b) provides additional criteria the Secretary of Commerce may consider in determining if an ICTS Transaction poses an undue or unacceptable risk but stops short of directly addressing industry's concerns with the past regulatory activity. According to Commerce's own analysis, the impact of the

January 2021 IFR will be felt by millions of firms, which will face compliance costs alone of up to $20 billion. BSA hopes that Commerce will take additional steps to reduce this impact and further the objective of supply chain security.

To respond to the specific question about the applicability of risk indicators contained in the NPRM: yes, the potential risk indicators should be applied to all ICTS Transactions under review if Commerce continues this approach. As Commerce notes, connected software applications were already contained within its definition of ICTS Transaction (a fact which this NPRM clarifies) and so these indicators should be applied to all ICTS Transactions, which has the added benefit of not further complicating this this rule.

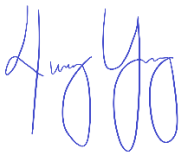
An Effective Path to ICT Supply Chain Security

BSA supports the goal of improving the security of information and communications technology and services, as well as protecting users' privacy, and BSA members are industry leaders in both developing and implementing cybersecurity and privacy solutions. BSA is optimistic that Commerce has identified a more specific subcategory of ICTS, i.e., connected software applications, and suggests Commerce continue to identify other more specific subcategories of ICTS and correspondingly limit the scope of the EO and IFR by redefining ICTS Transaction to include only the limited number of subcategories of ICTS that pose the type of undue or unacceptable risks identified in the EOs and subsequent regulatory actions.

BSA's White Paper, Building a More Effective Strategy for ICT Supply Chain Security identifies specific, assurance-based approaches that will lead to better security and economic outcomes. BSA would be pleased to discuss these approaches, and others, with the Department and other stakeholders to develop an effective plan to address the challenges identified in President Trump's EO on Securing the Information and Communications Technology and Services Supply Chain and President Biden's EO on Protecting Americans' Data from Foreign Adversaries. This approach could build a strong foundation from which the US Government, and governments around the world, can confront these challenges.

BSA is committed to working with the US Government, and governments around the world, to identify and address challenges discussed in the EOs and regulatory actions identified above. We look forward to this continued collaboration.

Sincerely,



Henry Young
Director, Policy

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org